

HARDWARE ENCRYPTION
NO SOFTWARE TO INSTALL
CROSS PLATFORM



1, 2, 4, 8 GB

SECURE STORAGE

HIGH SPEED

**30 MBPS READ
20 MBPS WRITE**

**HARDWARE
ENCRYPTION**

**WATERPROOF
TAMPER
RESISTANT**

THE WORLD'S MOST SECURE FLASH DRIVE

MEET IRONKEY BASIC.

The IronKey Basic is the world's most secure USB flash drive. Designed specifically for the needs of sensitive military, government and enterprise networks, it is extremely easy to deploy and use. IronKey Basic is the core technology platform for the IronKey family of secure storage and authentication products.

Always-On Data Encryption

All user data is encrypted with AES hardware encryption that has been validated to meet government FIPS requirements. Unlike software-based encryption, this "always-on" protection cannot be disabled. And since the Cryptochip generates and stores the strong, random encryption keys, the encryption routines run faster and more securely than any software-based encryption system.

Physically Hardened

The IronKey is an investment that will last for years. The IronKey has a rugged metal casing to protect it from physical damage, and the internal components are sealed to protect against tampering. Also, IronKey has passed and exceeded military waterproof testing requirements.

Secure and Effective

No one can access files stored on your IronKey unless they authenticate with the correct password. All encryption and password verification are performed in hardware, and cannot be disabled by malware or a careless user. This eliminates the risk of compromised confidential portable data.

Easy to Deploy and Maintain

The IronKey does not require any software or drivers to be installed and even works on Windows XP and Vista without administrator privileges. The IronKey offers drag-and-drop encryption, "plug and play" simplicity, and intuitive encrypted backup, which helps minimize the total cost of ownership. Onboard security software cannot be tampered with or removed. Each IronKey has a unique, easy-to-read serial number, making it simple to track and inventory.

Cross-Platform

IronKey Basic works with Windows 2000, Windows XP or Vista without administrator privileges or installing any software or drivers. Once initialized, IronKey Basic also works on Linux systems and on Macintosh OSX.

"This is without a doubt the most secure USB flash drive I've ever tested."
ComputerWorld February 2008

WHICH IRONKEY IS RIGHT FOR YOU?

	BASIC	PERSONAL	ENTERPRISE
Remote Management			✓
Configurable Policies			✓
OTP Strong Authentication			✓
Identity Protection Services		✓	✓
Security Software		✓	✓
Hardware Encryption	✓	✓	✓
Fast & Reliable Storage	✓	✓	✓
Tamper Resistant & Waterproof	✓	✓	✓

BASIC

TECHNICAL SPECIFICATIONS

Capacity

1GB, 2GB, 4GB or 8GB

Speed*

Up to 30 MB per second Read

Up to 20 MB per second Write

Dimensions

75mm X 19mm X 9mm

Weight

.9 oz (25 grams)

Waterproof

MIL-STD-810F

Temperature

Operating: 0 °C, +70 °C

Storage: -40 °C, +85 °C

Operating Shock

16G rms

Hardware

USB 2.0 high speed

OS Compatibility

Windows 2000, Windows XP, Vista

Linux & Mac OSX

Hardware Encryption

Data: AES Chained Block Cipher mode

Encryption Keys: 128-bit Hardware DRNG

PKI: 2048-bit RSA

Hashing: 256-bit SHA

FIPS validations: 140-2 Level 2, 186-2, 197

IRONKEY BASIC BENEFITS

- Enforces encryption policies
- Protects against lost and stolen flash drives
- Helps achieve policy compliance
- Easy to deploy and use
- No software or drivers to install
- No Windows administrative privileges required

SECURE, RELIABLE, EASY TO DEPLOY.

IronKey has worked with numerous enterprises and leading technology and security partners to provide an extremely secure solution that is reliable, easy to deploy, and will not increase calls to the Help Desk.

Reliable & Premium Quality

Encased in a solid, tamper-resistant and waterproof metal casing, the IronKey is built to survive years of wear and tear. IronKey only uses the highest quality components, yielding up to 10 times the average memory lifespan of a traditional flash drive.

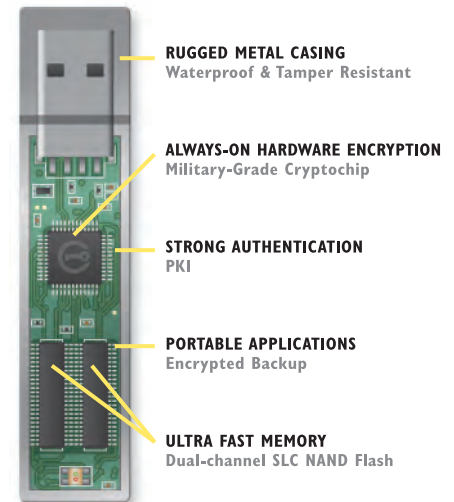
Hardware-Level Key Management and Defenses

When an IronKey is plugged into a laptop or desktop computer, the user must authenticate with a password before encryption keys are enabled and data and applications are accessible. Unlike software-based encryption, the IronKey Cryptochip does not export AES encryption keys to the host PC, thereby protecting against cold-boot and malware attacks.

The IronKey protects against brute-force password guessing attacks by using non-volatile access-failure counters stored on the Cryptochip itself. If a thief tries to break into an IronKey and enters 10 incorrect passwords, the Cryptochip securely erases all encrypted data with patent-pending Flash Trash technology. This ensures no data can be recovered from the device.

Endpoint Security Aware

The IronKey Basic has been designed to work seamlessly with many of the industry's leading endpoint security software products. Every device has a unique serial number, making it easy to manage and apply usage policies.



THE WORLD'S MOST SECURE FLASH DRIVE



www.ironkey.com
sales@ironkey.com
5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA



Secure By Design

IronKey's team of world renowned encryption, authentication, and Internet security experts designed IronKey devices and online services to withstand sophisticated security attacks, including brute force password guessing, USB sniffing, physical disassembly, differential power analysis and chip inspection.

©Copyright 2008 IronKey, Inc. All rights reserved. Reproduction in whole or in part without written permission from IronKey is prohibited. IronKey, Windows, and all other trademarks are properties of their respective owners. Features and specifications are subject to change without notice.

*Read/Write speeds tested in a laboratory environment. Actual speeds may vary. Advertised capacity is approximate. Not all of it will be available for storage.

IronKey Basic model numbers

1GB - D20103 ~ 2GB - D20203 ~ 4GB - D20403 ~ 8GB - D20803